
ACUA
WEBINARS

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website?

For more details, check out the Quick Tip post on

Connect.ACUA.org

Your Higher Education Auditing Connection

ACUA Kick Starters

Use a Kick Starter to launch your next audit!

- Developed by ACUA members with subject matter expertise
- Focused on higher education specific topics

https://acua.org/Audit-Tools/ACUA-Kick-Starters

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

Do you have a great idea for an ACUA Kick Starter? Contact Heather Lopez at hlopez@wsu.edu.

New Kick Starter Available!

Athletic Ticket Operations

Download today in the members-only section of www.ACUA.org

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Stay up to Date

- The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.
- News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

Connect with us

www.ACUA.org

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a conference proposal.
- Present a webinar.
- Write an article for the C&U Auditor.
- Become a Mentor.
- Write a Kick Starter.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Utilize Kick Starters
- Risk Dictionary
- Mentorship program
- NCAA Guides
- Resource Library
- Internal Audit Awareness Tool
- Governmental Affairs Updates
- Survey Results
- Career Center.....and much more.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of our upcoming conferences:

AuditCon
September 15-19, 2019
Baltimore Marriott Waterfront,
Baltimore, MD

- Contact ACUA Faculty for training needs.

WEBINAR MODERATOR

- Don’t forget to connect with us on social media!

ACUA Distance Learning Director
Amy L. Hughes
Director of Internal Audit
Michigan Technological University

Information Technology General Controls

Sudeshna Aich, MBA, CISA
Senior Information Technology Auditor
Office of Inspector General Services
Florida State University

Agenda

- **What are Information Technology General Controls (ITGCs)?**
- **Why perform ITGC audits?**
- **How to Audit ITGC?**
- **What are the Common Deficiencies and Findings?**

Almost 1 million UW Medicine patients' information exposed in data breach

Ga. university breach risks health, personal information of 417,000

A data breach at UConn Health may have compromised the personal information of about 326,000 people last year, the health center announced Friday.

UConn Health said "an unauthorized third party illegally accessed a limited number of employee email accounts," which contained the Social Security numbers of about 1,500 people and other personal information of the remaining 324,500 potentially impacted people.

Georgia Tech

April 2, 2019: Personal information of current and former faculty, students, staff and student applicants of Georgia Tech were accessed by a hacker through a central database. The database affected by the breach includes names, addresses, Social Security Numbers and birth dates of 1.3 million individuals. This is the university's second breach in less than a year.

wired.com/story/2018-worst-hacks-so-far/

WIRED The Worst Cybersecurity Breaches of 2018 So Far

how to respond. And while the state-sponsored hacking field is getting scarier by the day, you can use WIRED's grid-hacking guide to gauge when you should really freak out.

US Universities

In March, the Department of Justice indicted nine Iranian hackers over an alleged spree of attacks on more than 300 universities in the United States and abroad. The suspects are charged with infiltrating 144 US universities, 176 universities in 21 other countries, 47 private companies, and other targets like the United Nations, the US Federal Energy ommission, and the states of Hawaii and Indiana. The DOJ says the hackers

The Worst Cybersecurity Breaches of 2018 So Far

digital sphere, and the situation has been in a particularly delicate phase recently.

Rampant Data Exposures

Data breaches have continued apace in 2018, but their quiet cousin, data exposure, has been prominent this year as well. A data exposure, as the name suggests, is when data is stored and defended improperly such that it is exposed on the open internet and could be easily accessed by anyone who comes across it. This often occurs when cloud users misconfigure a database or other storage mechanism so it requires minimal or no authentication to access. This was the case with the marketing and data aggregation firm Exactis, which left about 340 million records exposed on a publicly accessible server. The trove didn't include Social Security numbers or credit card numbers, but it did comprise 2 terabytes of very personal information about hundreds of millions of US adults—not something you want hanging out for anyone to find. The problem was discovered by security researcher Vinny Troia and reported by WIRED in June. Exactis has since protected the data, but it is now facing a class action lawsuit over the incident.

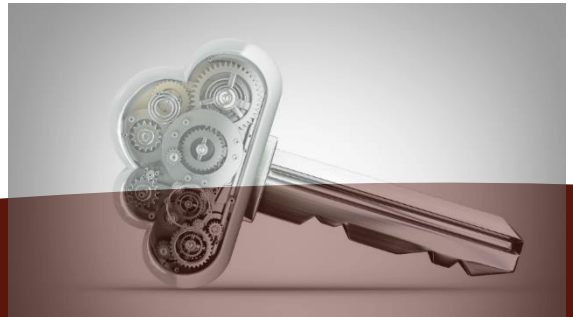
700,000 Choice Hotels records leaked in data breach, ransom demanded

Researchers found the unsecured database, but hackers got there first.

WHAT ARE ITGCs?

What are IT General Controls?

IT general controls (ITGCs) are the basic controls that apply to all the system components (such as applications, operating systems, databases), data, processes and supporting IT infrastructure. The objectives of ITGCs are to ensure the integrity of the data and processes that the systems support.



Primary Areas of ITGCs

- **ITGC Framework**
- **Access to Programs and Data**
- **Change Management**
- **Computer Operations**
- **Systems Development**

ITGC – Types of Controls

Preventive – Detective – Corrective

Preventive – prevent problems from occurring (Proactive)

- Segregation of Duties
- Monitoring
- Adequate Documentation
- Physical safeguards

Detective – identify problems after occurrence (Reactive)

- Logging and Monitoring
- Reviews

Corrective – prevent recurrence of problems

- Change controls as needed to eliminate error in future

How big is your audit shop:

1) 1 to 3 people
2) 4 to 6 people
3) 6 to 10 people
4) > 10 people

WHY PERFORM ITGC AUDIT?

Why perform ITGC audits?

- Determine Effectiveness and Efficiency of ITGC Controls
- Ensure controls related to Confidentiality, Availability, and Integrity of data and information are adequate
- Ensure Availability of mission-critical functions in a disaster situation
- Review Compliance with applicable polices, procedures, laws

Why perform ITGC audits?

- IT systems support many of the University's business processes, such as:
  - Student Records
  - Grading
  - Admissions
  - Finance
  - Purchasing
  - Human Resources
  - Research

We cannot rely on IT systems without effective IT General Controls

Example of FSU'S IT Environment

This is an example of IT environment at a major University

- 500 acres in Tallahassee
- 14,000 employees
- 41,000 students
- $1.7 Billion Operating Budget
- 40-50,000 Network Connections
- 4500 Wireless Access Points

MYFSU LINKS

Admissions

Advising

Alumni and Former Students

Benefits & Resources

Career Development

Financials

Human Resources

myFSU Identity Management

Reporting

Research

HOW TO PERFORM ITGC AUDITS?

ITGC – Audit Approach

- Understand and identify the IT Environment and systems to be reviewed
  - IT governance
  - Policies, procedures, guidelines
- Perform interviews, walkthroughs, and review documentation to gain an understanding on processes
  - Who performs what function
  - How something is done and documented

"If it is not documented, you did not do it"

ITGC – Audit Approach (Continued)

- Validate existing controls to assess control operating effectiveness
  - What are the major controls?
  - Are the controls working as intended?
  - Are the controls in-line with the University's IT security framework?
  - Are these controls reviewed periodically?
  - Who reviews these controls?

Does your organization have IT Security Policy?

1) Yes
2) No
3) Do not know

AUDITING IT GOVERNANCE AND FRAMEWORK

Why do we need to audit IT Governance and Framework?

- Obtain an understanding of IT Framework –
  - IT Security Policy, procedure, guidelines
- Determine if controls over University's IT structure are reasonable and oversight is adequate
  - IT reports and log
- Determine if IT operations are in-line with the University's strategies and objectives
  - IT reports and log

Example of Policy Objective (FSU)

4-OP-A-9 Internal Controls

Objective

The purpose of this policy is to provide guidance to help ensure the internal control objectives of the University are met. It is the responsibility of all University employees to ensure protection of University assets and resources. Administrators at all levels are responsible for establishing a strong control environment, setting the appropriate tone at the top, and displaying the proper attitude toward complying with these established controls

4-OP-H-5 Information Security Policy

Objective

The FSU Information Security Policy establishes a framework of minimum standards and best practices for the security of data and Information Technology (IT) resources at Florida State University

AUDITING ACCESS MANAGEMENT CONTROLS – COMMON TERMINOLOGIES

Access to Data

Data can be accessed via:

- Applications that create, edit, maintain and report data
- The network (Network domain administrators)
  - Data ‘In Transit’, ‘In Process’
- Primary servers (Server administrators)
  - Data ‘In Transit’, ‘In Process’
- Databases (Database administrators)
  - Data ‘At Rest’, ‘In Transit’, ‘In Process’

Access to Programs

User Access Management:

- User Access Provisioning
- Excessive Access
- Generic User ID and Privileged Access
- User Access Review
- User Access De-provisioning

Authentication

Authentication Controls

More powerful in terms of mitigating risk.

Authentication verifies that the login (ID/password) belongs to the person who is attempting to gain the access, i.e., users are who they say they are.

- Single Sign-on
- Multifactor Authentication

Authorization

Authorization controls

Act of checking to see if a user has the proper permission to access a particular file or perform a particular action, assuming that user has successfully authenticated.

- Credential focused
- Dependent on specific rules and access control lists preset by the network administrator(s) or data owner(s)

Physical Access Controls

Physical Access Controls

Limit access to buildings, rooms, areas, and IT assets.

- ID at the entrance
- Closing off access to laptops, desktops, and servers
- Safe structure for datacenter
  - Natural disasters – tornadoes, earthquakes, floods, and tsunamis.

Logical Access Controls

Logical Access Controls

Limits connection to computer networks, system files, and data to authorized individuals only and to the functions each individual can perform on the system. Logical security controls enable the organization to:

- Identify individual users of IT data and resources.
- Restrict access to specific data or resources.
- Produce audit trails of system and user activity.

Does your organization require periodic review of user access rights?

1) Yes
2) No
3) Do not know

AUDITING ACCESS MANAGEMENT CONTROLS

Why do we need to audit controls over User Access Management?

- To ensure:

  - IT Policies and procedures contain details about user management controls
    - Unique user IDs
    - Modification of existing user rights due to transfers or role changes
    - Disable and/or remove user accounts for terminated and transfer users
    - Periodic review of user access for all the users

Why do we need to audit controls over User Access Management?

- To ensure:
  - User access rights are appropriately requested, reviewed, and approved
  - User accounts are unique and not shared
  - All users and their activities are identifiable using unique user IDs
  - User access rights are in line with documented job requirement
  - Least-privileged access and need-to-know access for applications, databases, and servers is enforced

Why do we need to audit controls over User Access Management? (Continued)

- To ensure:
  - Only authorized users have access to confidential and sensitive information
  - Only authorized users have access to server room, datacenter
  - All users and their activities are identifiable using unique user IDs
  - Only authorized individuals have elevated privileges and their activities are logged and monitored:
    - System administrators
    - Database administrators
    - Network administrators

Why do we need to audit controls over User Authentication and Authorization?

- To ensure:
  - Authentication and authorization controls are addressed in detail in IT policies and procedures
  - Authentication mechanisms are enabled
    - Single Sign On
    - Multi-factor authentication
  - Password parameters are enforced for length, characters user, locking of computer screen when not used for certain time, password requirement to unlock the computer screen etc.
  - Vendor default passwords are modified

AUDITING CHANGE MANAGEMENT CONTROLS

Change Management

Change management is the process that ensures that all changes are processed in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure.

The main purpose of change management is to enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

Critical Points of Control in Change Management

- Evaluating Changes
- Authorizing Changes
- Testing Proposed Changes
- Moving Approved Changes into Production Environment

Why do we need to audit controls over the Change Management Process?

- To determine:
  - If a detailed change management policy and procedures exist
  - If the changes are appropriately reviewed, authorized, approved/rejected, and tested prior to implementing in production
  - If there is sign-off process, prior to a change moving into production, which includes information and documentation related to completion of quality assurance test, user acceptance test, approval for production implementation
  - If only approved changes are implemented
  - If changes have been implemented as planned

AUDITING COMPUTER OPERATIONAL CONTROLS

Computer Operations

Computer operations controls are designed to verify that the expected level of services will be delivered, and that the IT systems are functioning consistently, as planned.

- Monitoring the use of resources
- Monitoring the batch jobs
- Reviewing the job logs
- Monitoring the backup and recovery activities

Why do we need to audit controls over Computer Operations?

- To determine if:
  - Computer operations controls are in place to ensure systems and programs are available and operating as intended
  - Adequate physical safeguards, accounting practices, and inventory management over sensitive IT resources are in place
  - The University has appropriate processes and controls in place to continue its mission-critical functions with minimal disruption in case of an emergency or a disaster

Why do we need to audit controls over Computer Operations? (continued)

- To determine if:
  - The University has a Continuity of Operations and Disaster Recovery Plan
  - The University has identified the mission-critical functions for recover in disaster situation and the list is up-to-date
  - The University has a geographically separated location for backup and recovery

AUDITING SYSTEMS DEVELOPMENT CONTROLS

Systems Development

- The process of defining, designing, testing and implementing a new software application or program.
  - Internal development of customized systems
  - Creation of database systems or
  - Acquisition of third-party software

Systems Development Life Cycle

The primary phases in the development or acquisition of a software system are:

- feasibility study,
- requirements study,
- detailed design,
- programming,
- testing,
- Installation, and
- post-implementation review

Why do we need to audit controls over System Development?

- To determine if:
  - Detailed polices and procedures have been established for the systems to be developed, acquired or implemented, and for systems maintenance
  - Appropriate levels of authorization were obtained for each phase of the Systems Development Life Cycle
  - Adequate controls are in place for systems testing and the promotion of systems to production environments

Controls over Outsourced Services

Outsourcing is the process of contracting out one or more elements of operations to a supplier of services outside of the organization's management structure. A contractual arrangement is entered into at an agreed price with the supplier.

Why do we need to audit controls over Outsourcing?

- To determine if:
  - The University has an effective third-party management process
  - The University has a valid contract and a comprehensive service level agreement (SLA) with the third-party service providers
  - If the University is obtaining and reviewing service organization independent audit reports
    - SOC 2 audits under AICPA standards
    - ISO27001, Information Security Management Systems Requirements

COMMON DEFICIENCIES AND POTENTIAL RECOMMENDATIONS

Does your audit shop perform standalone IT audits?

1) Yes
2) No
3) Do not know

Deficiencies

- Terminated employees are still active in systems and the network
- There is a lack of segregation of duties over the development and production environments
- There is not a list of critical applications – no knowledge of vulnerabilities
- External penetration testing and internal vulnerability scanning are not conducted
- Shared and/or generic administrator accounts are not monitored
- System password parameters are not strong
- Disaster recovery plan is outdated and not tested
- Data backup is not tested
- There is no policy for portable device security

Potential Recommendations

- Entity IT security controls related to account management need improvement
- Some access privileges did not promote an appropriate separation of duties
- The entity did not perform comprehensive periodic reviews of access privileges for the application/server/database/network accounts
- The business continuity and disaster recovery plans continue to need improvement to ensure that critical operations continue in the event of a disaster or other interruption of service

ITGC Controls Currently Being Reviewed by FSU's IT Office

- Change Management
- Emergency Change Management
- IT Governance
- Vulnerability Management – ERP and Infrastructure
- Software Development Life Cycle Review
- User Provisioning
- User Terminations and Transfers
- Oracle DBA Entitlement Review
- Windows Domain Administrator Entitlement Review
- Security Awareness Training
- Disaster Recovery Plan Updates
- Policy Review - Security, Privacy, Acceptable Use
- Review of ITS access to SSN/Protected Information

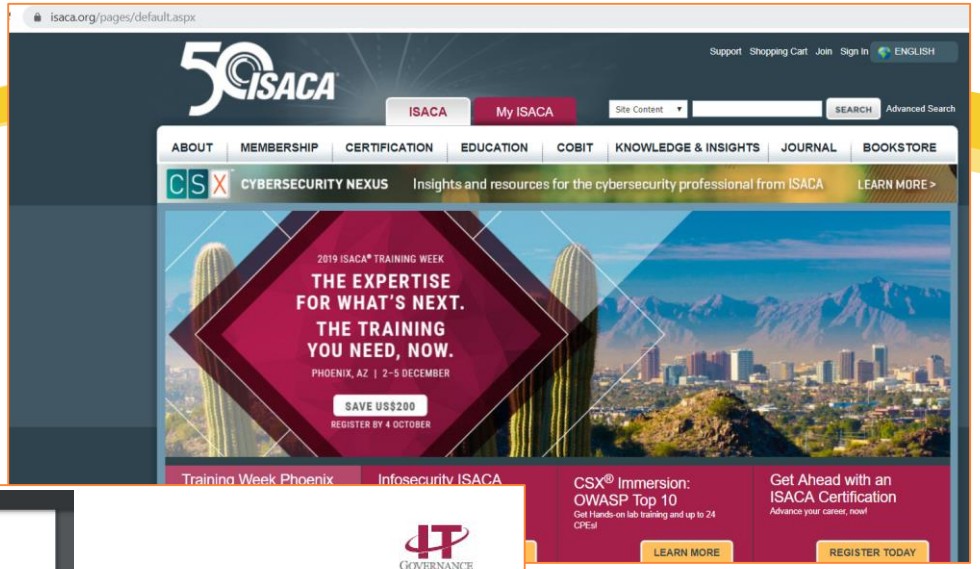
ITGC Audit Program

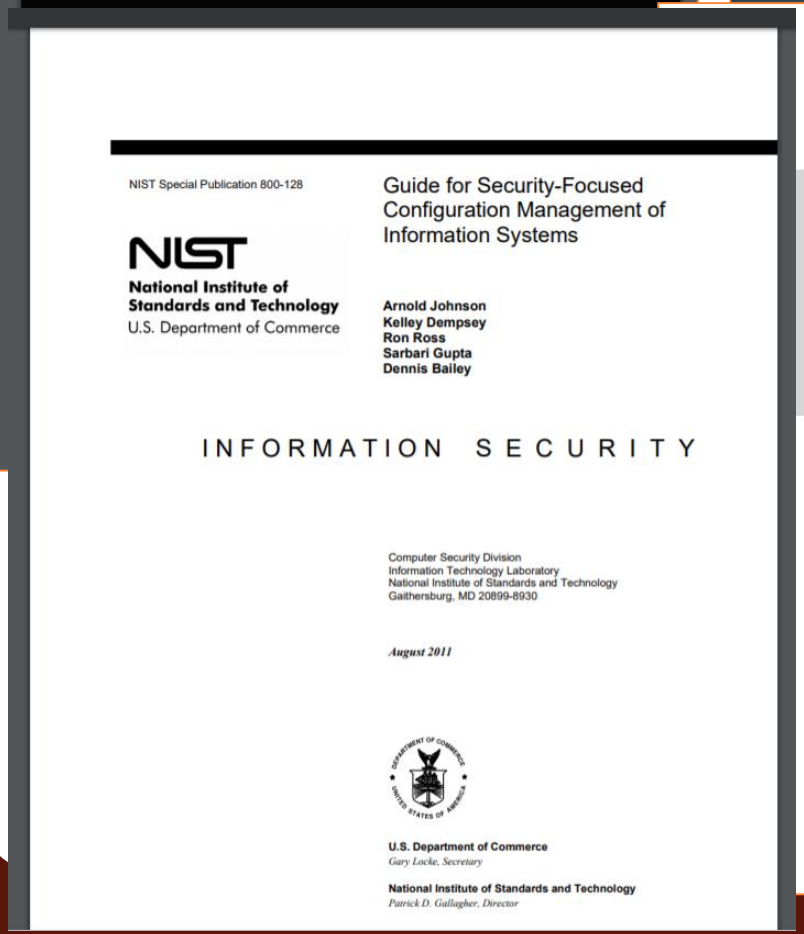
A detailed list of audit objectives and methodologies and common findings are provided in the handout:

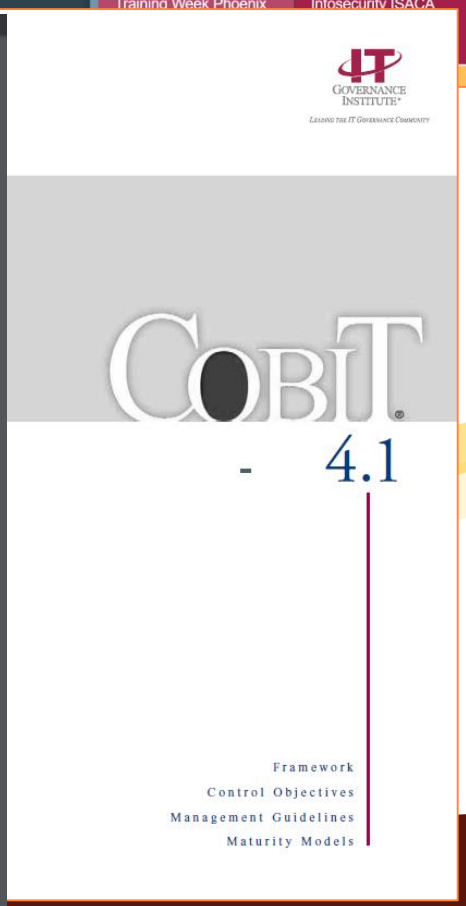
- IT General Control Audit Program

STANDARDS GUIDELINES AND BEST PRACTICES


GTAG
GLOBAL TECHNOLOGY AUDIT GUIDE
IPPF – Practice Guide
Information Technology Risk and Controls
2nd Edition


isaca.org/pages/default.aspx
ISACA
Support Shopping Cart Join Sign In ENGLISH
ISACA My ISACA
Site Content SEARCH Advanced Search
ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE & INSIGHTS JOURNAL BOOKSTORE
CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA LEARN MORE >
2019 ISACA® TRAINING WEEK
THE EXPERTISE FOR WHAT'S NEXT.
THE TRAINING YOU NEED, NOW.
PHOENIX, AZ | 2–5 DECEMBER
SAVE US$200
REGISTER BY 4 OCTOBER
Training Week Phoenix
Infosecurity ISACA
CSX® Immersion: OWASP Top 10
Get Hands-on lab training and up to 24 CPEs!
LEARN MORE
Get Ahead with an ISACA Certification
Advance your career, now!
REGISTER TODAY


NIST Special Publication 800-128
Guide for Security-Focused Configuration Management of Information Systems
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Arnold Johnson
Kelley Dempsey
Ron Ross
Sarbari Gupta
Dennis Bailey
INFORMATION SECURITY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930
August 2011
U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Director


IT GOVERNANCE INSTITUTE
Leading the IT Governance Community
COBIT
4.1
Framework
Control Objectives
Management Guidelines
Maturity Models


Start Secure. Stay Secure.®
CIS Center for Internet Security®
CIS Controls™
V7.1

ITGC – Resources

https://na.theiia.org/standards-guidance/Member%20Documents/GTAG-1-2nd-Edition.pdf

https://www.iia.org.uk/resources/auditing-business-functions/supply-chains/outsourced-services/?downloadPdf=true

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Change-Management-Audit-Assurance-Program.aspx

https://www.cisecurity.org/controls/cis-controls-list/

Thank you!

Upcoming ACUA Events

September 15-19, 2019

AuditCon in Baltimore, MD - **Registration is closed but you may still register on-site. Visit the ACUA website for details.**

October 3, 2019

Using the ACUA Kick Starter to Audit IT System Access Controls

October 17, 2019

Climbing the ranks: Best practices for preventing fraud and misreporting in admissions and institutional data


ACUA
WEBINARS
Join us for
our upcoming
webinar.